МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Н. Ф. Ржевська
«____»_____ 20 __ р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГСОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ОСОБЛИВОСТІ ІНФОРМАЦІЙНИХ ВОЄН»

Виконавець: студент 4 курсу, 409 групи, Цибенко Даніїл Олександрович

Керівник: кандидат історичних наук, доцент кафедри міжнародних відносин, інформації та регіональних студій Дерев’янко Ігор Петрович

Нормоконтролер _____ _____
(підпис) (П.І.Б.)

КИЇВ 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЗМІ – Засоби масової інформації

США – Сполучені Штати Америки

ЗС - Збройні сили

ЗСУ – Збройні сили України

ООС - Операція об’єднаних сил

АТО - Антитерористична операцію

РФ – Російська федерація

ВСТУП

Кінець XX століття ознаменувався появою нової зброї, яка виявилася потужнішою і більш дієвою, а головне – такою, що не несе загрози фізичної, як звичайна зброя. Інформаційні війни, велися з найдавніших часів. Однак в далекому минулому люди вміли впливати на одне одного в процесі безпосереднього спілкування, впливаючи на своїх співрозмовників за словами, інтонацією, жестами, мімікою.

Актуальність. Актуальність досліджень у сфері інформаційних воєн, багатогранність форм і методів цієї роботи в науковому та практичному планах визначається тим, що сьогодні будь-яка країна світу потребує створення ефективної системи державної протидії інформаційної війни, прояву її різних форм. Наразі багато держав розглядають інформаційну війну як ефективний інструмент реалізації своєї зовнішньої політики.

На сьогоднішній день вплив на людську свідомість став набагато різноманітним, дієвим і витонченим завдяки накопиченому за тисячоліття

практичному досвіду. Тому інформаційна війна – це не що інше, як явні й приховані цілеспрямовані інформаційні впливи систем одне на одного, на меті якої є отримання певної користі. Враховуючи наведене визначення інформаційної війни, застосування інформаційної зброї означає, перш за все, роботу з громадською думкою, з ідеологією противника.

Для відсічі інформаційної агресії необхідно, перш за все, розуміння суті того, що відбувається. Наразі здійснюється глобальна інформаційно-культурна й інформаційно-ідеологічна експансія Заходу, що здійснюється по телекомунікаційних мережах, через Інтернет і засоби масової інформації.

У багатьох країнах приймають спеціальні заходи для захисту своїх співгромадян, культури, традицій і духовних цінностей від чужого інформаційного впливу.

На підґрунті необхідності захисту національних інформаційних ресурсів та збереження конфіденційності інформаційного обміну, можуть виникати політичні та економічні конфронтації держав, нові кризи в міжнародних відносинах. Тому інформаційна безпека, інформаційна війна і інформаційна зброя наразі опинилися в епіцентрі загальної уваги.

Метою дипломної роботи є вивчення природи і технології інформаційної війни як форми інформаційної влади над суспільством і державами, безконтрольність і некерованість яких може призвести не тільки до масового винищення окремих народів, а й до загибелі сучасної цивілізації в цілому.

Поставлена мета зумовила виконання наступних **завдань**:

1) визначити основні поняття й підходи до вивчення політичного інформаційного простору;

2) охарактеризувати концепції «інформаційної війни» у вітчизняній та зарубіжній політології ;

3) розглянути інформаційні війни на сучасному етапі: форми, види і методи їх ведення;

4) проаналізувати проблему інформаційної безпеки України в умовах сучасних інформаційних війн;

5) визначити загрози безпеці України в інформаційній сфері;

6) з'ясувати механізми забезпечення інформаційної безпеки України.

Об'єктом дослідження є комплексні інформаційні потоки, що представляють основу такого явища як сучасні інформаційні війни.

Предметом дослідження – форми, види і способи ведення інформаційних війн.

Теоретичну базу дослідження складають книги Почепцова Г. Г. «Сучасні інформаційні війни», Расторгуєва С. П. «Інформаційна війна», Панарина І. П. «Інформаційна війна і третій Рим». До уваги також візьмемо зарубіжні літературні джерела: книги Тоффлера Е. «Третя хвиля», М. Лібікі «Що таке інформаційна війна?», котрі дозволили краще зрозуміти й інтерпретувати витоки і передумови настання інформаційної ери, і як наслідок – інформаційного протиборства.

Методологічна база дослідження – політологічний метод, загальнонаукові методи: аналіз, синтез, системний і структурно-функціональний підходи, історичний і логічний методи.

Гіпотеза дослідження полягає у припущенні, що методи і прийоми ведення інформаційної політичної війни в міжнародних справах згубно впливають на соціум, породжуючи ненависть між народами. Прийоми психологічного тиску різні, але їх політичний сенс має один спільний знаменник: утримання влади за всяку ціну.

Структура роботи відповідає поставленим завданням і складається з вступу, трьох основних розділів, висновків, списку використаної літератури.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Основні поняття і підходи до вивчення політичного інформаційного простору

У наш час інформація стала формуючим фактором у матеріальному середовищі людського життя, і вона виступає в ролі інноваційних технологій, комп'ютерних програм та інших ролей. Водночас він використовується як основний засіб людської взаємодії, постійно з'являється і замінюється під час переходу від однієї інформаційної системи до іншої. Цей статус інформації в суспільстві ставить за необхідне розглядати її як продукт із певною цінністю, яка зростатиме із підвищенням надійності, практичності та зручності використання.

Від латинського термін «інформація» походить перекладається буквально: ознайомлення, уявлення, роз'яснення, поняття. У більшості наукових праць з проблем інформаційної безпеки, поняття інформація не формується.

В Україні необхідність створення інформаційного суспільства ставить перед державою завдання перегляду напрямків формування інформаційного простору. При цьому слід зважати на світовий досвід й ті зміни, що відбуваються в умовах глобалізації. Питання створення інформаційного простору потребує створення системи національних інформаційних ресурсів, забезпечення підвищення рівня інформаційної незалежності держави, підвищення рівня інформаційної культури, розповсюдження відомостей про стан розвитку інформаційного простору України в Інтернеті. При цьому варто покращувати ефективність функціонування всіх гілок влади державного управління та самоврядування на основі використання

нагромаджених інформаційних ресурсів та більш динамічної організації інформаційної взаємодії під час вирішення складних проблем [22].

Наразі в суспільстві немає жодної сфери діяльності людини, яка б не була пов’язана з інформацією, її створенням, обробкою і передачею. Чим більш розвинене суспільство, тим більше в ньому працівників, які займаються інформаційною діяльністю. Необхідність створення загального інформаційного простору випливає із вимог часу і прагнення нашої держави увійти у світовий інформаційний простір.

Інформаційний голод майже в усіх сферах державного правління позначився на прийнятті великої кількості нормативних актів, що регламентують інформаційний простір, проте містять різну термінологію. Тому, вважаємо, що першочерговим завдання у дослідженні інформаційного простору України усунення суперечностей у тлумаченні основних дефініцій, а також визначення головних підходів щодо дослідження інформаційного простору [53, с. 30].

Поняття «інформаційний простір» і різні його аспекти широко вивчені в контексті різних сфер діяльності як з теоретичної, так і з практичної точок зору.

Поява поняття інформаційний простір обумовлено потребою суспільства в безперервному інформуванні. Крім того, формування «інформаційного суспільства» тісно пов'язане із упровадженням новітніх технологій, за допомогою яких інформація до аудиторії надходить значно швидше.

Різні підходи до вивчення поняття «інформаційний простір» представлені в роботах багатьох вітчизняних і зарубіжних науковців.

Вже кілька десятиліть, тема захисту і розвитку національного інформаційного простору є приводом для наукових дискусій. Її

розробниками вважаються такі закордонні фахівці, як А. Моль, М. Кастельс, Д. Томпсон, З. Бжезинський, , Ф. Вільямс та багато інших.

З проголошенням незалежності нашої держави цю проблематику досліджують й українські науковці. Вони значну увагу приділяють питанням інформаційного простору України, його становленню, проблемам та перспективам функціонування. На особливу увагу в цій сфері заслуговують праці А. Москаленка, П. Шевчука [54], В. Здоровеги [17], І. Михайліна, В. Карпенка [24], Г. Кривошеї та Ю. Горбаня [11]. Зокрема, вплив інформаційних технологій на розвиток засобів масової інформації знаходимо у дослідженнях таких науковців як О. В. Зернецької, О. Мелещенко, В. Різун [47].

У свою чергу О. В. Литвиненко, О. Пантелеймонов, О. Соснін вивчали процеси національної ідентифікації та національної безпеки інформаційних просторів в умовах глобалізації інформаційного простору. Правовим аспектам інформаційної галузі присвячені розвідки В. Іванова [20]. Крім того, інформаційний вплив на масову свідомість досліджував Г. Почепцов [42; 43; 44; 45].

Серед російських вчених у цій галузі вважаємо слід відзначити таких науковців як С. Є. Зуєв («Вимірювання інформаційного простору: політики, технології, можливості»), С. А. Модестов («Інформаційне протиборство як фактор геополітичної конкуренції»), С.П. Расторгуєв («Інформаційна війна») [46], І. М. Дзялошинский («Глобалізація медіапростору і проблеми культурного розмаїття»), А. І. Ненашев («Інформаційний простір сучасного суспільства: комунікаційний аспект»), А. В. Манойло («Державна інформаційна політика в особливих умовах») [31], В.Г. Машликін («Європейський інформаційні простір»).

Під інформаційним простором прийнято розуміти територію поширення інформації за допомогою конкретних компонентів системи

інформації і зв'язку. До таких компонентів варто віднести: матеріальні (технологічні) можливості поширення інформації з горизонталі й вертикалі, її передачі в будь-яких напрямках та наявність регіональних і міждержавних угод, заснованих на розумінні того, що жоден із процесів інформації не може розглядатися як феномен винятково національного характеру. Спеціальними параметрами інформаційного простору можуть стати: загальна кількість засобів масової комунікації, загальний обсяг її продукції, яка розповсюджується і приймається на даній території; опосередкована фіксація тих або інших результатів контакту із продукцією реципієнтів засобів масової комунікації [6, с. 74].

Інформаційне середовище являє собою сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації. Інформаційне середовище можна визначити як ту частину інформаційного простору, яка формує найближче інформаційне оточення індивіда, виступає як сукупність умов, що певною мірою забезпечують його продуктивну діяльність. Цілі такої діяльності визначає те інформаційне середовище, яке обирає людина.

Дуже важливим постає питання правового статусу інформаційного простору України як основи правового регулювання захисту національних інформаційних ресурсів. Зважаючи на наявні нині небезпечні тенденції заперечення можливості управління інформаційним політичним простором, які пояснюються відкритістю його та домінуванням у ньому країн-лідерів у сфері інформаційних технологій, проблема формування національного інформаційного простору є важливою умовою гарантування державного суверенітету нашої країни. А отже, дуже вагомим є науково обґрунтоване та юридично точне визначення цього поняття.

Існують різні підходи до вирішення цього питання. У монографії О. Литвиненка «Інформаційний простір як чинник забезпечення національних інтересів України» визначають так: «Під національним інформаційним простором будемо розуміти всю сукупність інформаційних потоків як національного, так й іноземного походження, які доступні на території держави. » До них відносять потоки, що формує преса, електронні ЗМІ, та які циркулюють в інформаційних мережах тощо [17, с. 8].

Вивчаючи сферу діяльності інформаційних агентств в умовах формування глобального комунікаційного простору, російський вчений О. Пантелеймонов відзначає слабку інтегрованість України у світовий інформаційний простір, використання інформаційного вакууму країни для підриву її авторитету в світі, нав'язування цінностей і стереотипів Заходу та інші численні інформаційні загрози її національній безпеці. Науковець стверджує, що наразі вплив глобального інформаційного простору на національний простір нашої держави вирізняється динамічністю та складністю, причому міжнародні інформаційні агентства зазнають більшого впливу і конкуренції з боку інших потужних утворень у цій сфері, до числа яких входять деякі з найбільших світових газет, низка телевізійних систем мовлення, найбільші світові журнали, телевізійні і фінансові інформаційні агентства, потужні медіа конгломерати тощо. Тому Україні необхідно створювати власну систему інформаційних агентств і розробляти конструктивні дії щодо створення адекватної правової бази для забезпечення поточної діяльності цих утворень [50].

У зв'язку з цим, дослідник О. Соснін переконаний, Україна має освоїти глобального інформаційного простору, що має стати стратегічно орієнтованою діяльністю країни у напрямку нового інформаційного середовища. Оскільки глобальний інформаційний простір як середовище існування і функціонування народів і держав здатний як забезпечити країну

великими ресурсами, так і призвести до зникнення національної культури, втрати народами своєї національної самоідентифікації [50, с. 93].

Науковець так зазначає, і з ним важко не погодитися, що до тепер чинне законодавство не визначило правового статусу інформаційного простору України, що є важливу рисою й передумовою формування інформаційного суверенітету України. До речі, це право О. Соснін тлумачить як виключне право держави, згідно з Конституцією та законодавством, а також відповідно до норм міжнародного права, самостійно й незалежно, з дотриманням рівноваги інтересів особи, суспільства і держави визначати і здійснювати внутрішні й геополітичні національні інтереси в інформаційній сфері, внутрішню й зовнішню інформаційну державну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру державного інформаційного простору, створювати умови для його об'єднання у світовий інформаційний простір та гарантувати інформаційну безпеку держави [50, с.167].

У свою чергу, український науковець в галузі комунікаційних процесів Г. Почепцов зауважує, що «наразі Україна не надає значення новим реаліям інформаційного суспільства. У нас немає академічних інститутів, які працювали б у цьому напрямі, ми всі ще готуємо фахівців винятково однієї сфери – журналістів. Вони не є аналітиками, вони не можуть розробляти інформаційних кампаній, вони не можуть працювати в галузі зв'язків з громадськістю. Немає підготовки відповідних фахівців ні в цивільних, ні у військових вузах, немає необхідної підтримки в академічному середовищі. Болгарія, наприклад, має свій власний журнал з інформаційної безпеки, не кажучи вже про США, де друкуються десятки книг, де військових перенавчають новим реаліям інформаційної війни, що змінює всю стратегію й тактику, напрацьовану в минулому» [42, с.163].

Всі дослідники, що вивчають інформаційний простір України, вважають, що необхідний активний розвиток інформаційної інфраструктури українського суспільства. Він можливий за умови наявності виразної, зрозумілої й прийнятої програми такого розвитку. В державі має бути створена відповідна «Концепція реформування інформаційної інфраструктури», яка повинна найретельнішим чином сконцентрувати такий досвід, щоб реформувати власну інформаційну інфраструктуру. Оскільки без її адекватного функціонування неможливий подальший економічний, політичний, демократичний розвиток України [40].

В умовах інформатизації суспільства інформаційний вплив на особистість набуває глобальних масштабів, що можуть набувати загрозливих ознак. Інформаційні загрози ретельно аналізує у своєму дослідженні російський науковець Я. Жарков. Він тлумачать їх як сукупність умов і факторів, які створюють небезпеку життєво важливим інтересам особистості, суспільства, держави в інформаційній сфері. Технічні пристрої, за допомогою яких здійснюється інформаційний вплив на особистість, суспільство і державу в ході інформаційного протиборства (інформаційна зброя), дослідник наводить деякі найчастіше вживані в публікаціях її визначення – від дезінформації й пропаганди, до засобів радіоелектронної боротьби [16, с.42].

Проте українська вчена О. Буньківська вважає, що зараз змінився сам підхід до організації інформаційно простору: якщо раніше ми говорили про формування інформаційного простору, то сьогодні – про його моделювання й оптимізацію. Це пов’язано насамперед з істотними матеріальними витратами в процесі супроводу інформаційного простору, значна частина яких містить витрати на придбання технічного оснащення, навчання й підготовку фахівців, розробку й упровадження програмного забезпечення [7].

Розширення інформаційного простору й підвищення його значення в житті людей призводить до формування нового життєвого простору як

цілісного поля, усередині якого перебувають взаємодіючі між собою індивіди. Специфіка його полягає в розірваності двох рівнів буття: реального й віртуального, а тому породжує нові норми й ситуації існування. Здобуваючи глобальний характер, інформаційні технології сприяють розширенню комунікацій і формуванню єдиного інформаційного простору, у рамках якого виробляються особливі закони й норми поводження і світосприймання.

Основними характеристиками інформаційного політичного простору є протяжність простору (контрольованими державою безпосередньо чи опосередковано – каналами інформації користуються практично всі громадяни незалежно від регіону проживання), упорядкованість (наявність сукупного тексту вітчизняних мас-медіа, постійне підтримання основного масиву інформації), інтенсивність інформаційних процесів. Через відсутність якісної технічної бази доводиться констатувати телевізійну інтервенцію в Україні. За таких умов неможливо створювати національний інформаційний простір, який би зміг протистояти іноземній інформаційній експансії, коли відбувається гіпертрофоване розростання інформаційного простору держави з потужнішою індустрією мас-медіа [6, с. 70].

Інструментальні засоби завжди супроводжували розвиток суспільства. Поява певних принципових технічних інновацій в системі виробництва рано чи пізно призводила до радикальних соціальних та духовно-культурних трансформацій. Саме інформаційні комунікації стали постійною рушійною силою, яка вносила кардинальні зміни у розвиток суспільства.

Отже, сьогодні Україна перетворилася на заручника глобалізаційного процесу. Як відповідь на історичні виклики третьої цивілізаційної хвилі, процес входження її у світовий інформаційний простір є досить пасивним, що супроводжується лише використанням окремих компонентів та технологічних рішень з арсеналу інформаційного суспільства. Хоча швидкий

розвиток технологій та впровадження нових технологічних рішень принципово змінили інформаційний ландшафт країни, його сегментація з технологічної, соціально-економічної та політико-ідеологічної точок зору є противагою потребі консолідації національної держави. Нерозвиненість інформаційної складової державного управління створює неефективну модель комунікативних зв'язків між владою та суспільством.

1.2. Концепції «інформаційної війни» у вітчизняній та зарубіжній політології

XXI століття як правило називають «ерою інформаційних технологій». Це й не дивно, адже зараз відбувається колосальний розвиток у сфері розробки методів і засобів ведення інформаційної війни, а також боротьби з нею. За таких умов інформаційна безпека стала мало не панацеєю при вирішенні проблем інформаційного суспільства.

Сьогодні чимало держав надають особливого значення розвитку новітніх технологій, а також інформаційної безпеки своєї держави, адже усвідомлюють важливість впливу ЗМІ на масову свідомість на різних рівнях, регіональному, міжнародному тощо.

Сучасні науковці О.О. Зінов'єв [18], І. Костюк [26], В. М Коровін наголошують, що війна вже йде. Але це та війна, що не оголошується на офіційному рівні, і, як правило, прихована від погляду пересічних громадян. Проте вона веде країни до глобальних змін, відповідно до їх розстановки на міжнародній арені. Феномен такої «прихованої» війни можливий тільки за умов розвитку інноваційних інформаційно-комунікаційних технологій.

Аналіз світового досвіду засвідчує: зараз пряма агресія перестала бути основним засобом домінування. У зв'язку з цим сучасна наука поступово

зосереджується на вивченні непрямих форм боротьби, приділяючи особливу увагу інформаційним війнам.

«Інформаційна війна» – термін, що наразі носить здебільшого публіцистичний характер і досі не отримав сталого визнання. Свідченням цього є неперервні дискусії і суперечки стосовно того, що насправді криється під цим поняттям. До того ж виникає полеміка з приводу коректності та практичного застосування терміну до тієї сфери соціальних відносин, яку прийнято називати інформаційною боротьбою або конфліктом інтересів в інформаційній сфері соціальних систем [25].

Таким чином, окремою науковою проблемою вважаємо розробку і узгодження науково-термінологічного апарату щодо визначення поняття інформаційної війни.

Сьогодні у зарубіжній та вітчизняній науці є багато підходів щодо визначення конфліктів у сучасному інформаційному просторі. Часто вони є взаємовиключними. Утім така різноманітність і неузгодженість є суттєвою перепоною на шляху щодо опрацювання теорії інформаційних війн.

Дослідження інформаційної війни знайшло відображення в фундаментальних наукових розвідках відомих аналітиків, таких як Г. Почепцов [42; 43; 44; 45], В. Разуваєв, Г. Тульчинський, В. Кноріг, Л. Козер, І. Панарін [36; 37], С. Завадський, Г. Афанасьєва, З. Бжезинський, Г. Ласвель, Г. Карпенко [24] та ін.

Термін «інформаційна війна» вперше вжив Томас Рона в звіті «Системи зброї й інформаційна війна», підготовленому ним 1976 року [21]. Він наголошував, що інформаційна інфраструктура є головним аспектом американської економіки, водночас вона стає і вразливою ціллю як у воєнний, так і в мирний час.

Однак на думку російського науковця І. М. Панаріна, щодо введення даного терміну варто рахувати не 1976 р., а 1967 року, коли А. Даллес

(головний організатор інформаційної війни проти Радянського Союзу) видав книгу «Таємна капітуляція», присвячену таємним сепаратних переговорам між США і Великобританією, з одного боку, і рейхсфюрером СС Гіммлером – з іншого. Саме у ній вперше вводився термін «інформаційна війна», який включає особисті, розвідувальні, диверсійні дії по підриву тилу противника [36, с.184]. Згодом це поняття стало активно вживатися в пресі, здебільшого після проведення в 1991 році операції «Буря в пустелі».

Наразі поняття «інформаційна війна» визначається по-різному. Це пов'язано з багатозначністю терміну «information warfare», що породило купу різночитань при його перекладах.

Даний термін може тлумачитися як «інформаційна війна», «інформаційне протиборство», «інформаційно-психологічна війна». Для прикладу, інформаційна війна визначається як інформаційна діяльність, що вживається політичним утворенням (наприклад державою) для ослаблення, знищення іншого політичного утворення; як інформаційна боротьба між учасниками змагання; інформаційний військовий конфлікт між двома масовими ворогами, наприклад арміями тощо [39, с. 112].

Теоретичний аналіз засвідчив, що наразі існує безліч переконливих концепцій інформаційної війни, однак загальноприйняте визначення даного поняття поки відсутнє. Це зумовлене передусім складністю самого об'єкта дослідження, а також теоретичними і методологічними позиціями авторів, що належать до різних наукових шкіл і акцентують увагу на певних аспектах проблематики.

З точки зору психологічної парадигми інформаційна війна визначається як прихований вплив інформації на персональну, групову і масову свідомість за допомогою методів пропаганди, дезінформації, способів маніпулювання задля формування нових поглядів на соціально-політичну

організацію суспільства через зміну вартісних орієнтацій і базових установок особистості.

Досліджуючи інформаційну війну в контексті психологічних теорій, В. А. Лисичкін і Л. А. Шелепін вказують, що об'єктом є когнітивно-емоційна сфера індивідів, а головною метою – управління інтелектуально-психологічними та соціокультурними процесами. Основним елементом такого управління є неусвідомленість такого впливу особами, схильними до завуальованого впливу й поведінка яких легко програмується [15].

Психологічний вплив зазначеного феномена інтерпретують також Д. А. Волкогонов [9], М.І. Живейнов та А. Г. Караяні [23]. Вчені поєднують в одному понятті інформаційне та психологічне протиборства. У свою чергу, Д. Волконогов розглядає інформаційну війну в якості системи підривних ідеологічних впливів імперіалізму, спрямованих на свідомість людей переважно через сферу соціальної психології [9 с. 47]. Натомість А. Г. Караяні переконаний, що мова йде про інформаційно-психологічні акції, які здійснюються на міждержавному, стратегічному, оперативному й тактичному рівнях, як в мирний, так і у воєнний час, як в інформаційній, так і в духовній сфері, серед своїх військовослужбовців або військ противника [23, с. 107].

Проблеми інформаційних війн, котрі розкривають сутність процесів інформаційного впливу на суспільство знаходимо у працях І. Костюка [26], О. Саприкіна [48], П. Шевчука [54].

А от В. Карпенко, досліджуючи український інформаційний простір, деталізує інформаційну експансію Росії, яка поширює неоімперіалістичні ідеї й форми російської експансії подає в інформаційному просторі України, через українські засоби масової інформації [24, с. 182].

Актуальним, на нашу думку, є геополітична концепція, відповідно до якої інформаційна війна інтерпретується в поняттях міждержавного

протиборства, спрямованого на вирішення зовнішньополітичних цілей без застосування фізичної сили, військової техніки і зброї, а за допомогою витончених технологій контролю, що має зовнішнє вираження у формі дипломатії. У цьому напрямку заслуговують на увагу дослідження І. А. Михальченка. Науковець відстоює позицію, згідно з якою інформаційна війна визначається як цілісна технологія, спрямована на досягнення гуманітарного поневолення одних груп людей іншими. Вона є продуктом постіндустріального суспільства і обумовлена неможливістю глобальних збройних конфліктів, які можуть знищити планету [34, с.15].

Прибічником такого підходу є російський політолог І. М. Панарін. За визначенням науковця, інформаційна війна – це «домінуючий спосіб досягнення влади, організації ноосфери і світового інформаційно-психологічного простору у власних інтересах» [34, с. 104]. На його думку, сучасні державні діячі не тільки повинні мати та володіти владним ресурсом і кредитом довіри громадськості, а й вести ефективне інформаційне протиборство. Саме така позиція збільшуватиме політичний капітал політика.

Згідно з концепцією І.М. Панаріна, інфовійна – термін, що має два значення. Він також використовує термін «психологічна війна».

Перше значення тлумачить термін як психологічний вплив на цивільне населення і (або) військовослужбовців іншої держави з метою досягнення політичних або чисто військових цілей.

Другий – цілеспрямовані дії, застосовані для виконання інформаційної переваги шляхом завдання шкоди інформації, інформаційним процесам та інформаційним системам супротивника водночас при захисті власної інформації, інформаційних процесів та систем.

Наразі ж сучасних наукових дослідження виокремлюється коло вчених, які концентрують свою увагу на соціально-комунікативному аспекті

інформаційних воєн. Їх методологічні принципи дослідження відрізняються тим, що в предметному полі домінує інформація, що набуває панівного впливу у sms реальності і формує лише когнітивні орієнтації, а не свідомість людей.

Прихильниками цієї концепції є М. Ю. Павлютенкова і Д. А. Швець. На їхню думку, інформаційна війна представляє собою комунікативну технологію, котра має на меті досягнення інформаційної переваги в інтересах національної стратегії [35, с.23; 53, с. 34].

Викликають інтерес до зазначеної проблеми і розвідки П. Шпиги та Р. Рудника, у яких науковці виокремлюють 4 підходи до визначення даного поняття. Перший підхід тлумачить їх як комплекс політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, повалити ворога з інформаційної сфери, ліквідація його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі.

Другий роз'яснює інформаційну війну як найгострішу форму протистояння в інформаційному просторі, де першочергового значення набувають безкомпромісність, висока інтенсивність сутички та короткотривалість гострого суперництва.

Третій підхід інтерпретує інформаційну війну як форму забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів (цифрових випромінювачів, супутників й інших інноваційних технологій), які застосовуються для виконання військових завдань.

Четвертий підхід інтерпретує інформаційні війни з кібернетичними війнами (протистояння між технічними системами). Поза увагою не можна залишити ідеї конфліктологічного підходу, що дозволяє розглядати аналізовані війни в ракурсі військового і політичного протистояння [55, с. 328].

Отже, наведені підходи концепції інформаційної війни дають можливість сформувати уявлення про окремі сторони досліджуваного явища.

Психологічна парадигма дозволяє детально досліджувати механізми впливу на внутрішньоособистісні процеси людей, що викликає зміни в їх ментальній сфері, визначає корекцію логіки світосприйняття і відповідної політичної поведінки.

Геополітичний підхід дозволяє розглядати основні методи сучасної світової політики для досягнення політичного та економічного панування в мирний період.

Конфліктологічний напрямок орієнтує на адекватну оцінку стратегічного значення інформації в досягненні домінуючих позицій як результату боротьби за владу, ресурси та політичний статус.

Системний підхід дає релевантний інструментарій для комплексного вивчення інформаційної війни з урахуванням тісного взаємозв'язку її окремих елементів, їх рефлексії на дестабілізуючі чинники і тактики в рамках наступальних стратегій.

Таким чином, інформаційна війна є багатоплановим і достатньо складним феноменом, що ведеться в різних вимірах. Тому вважаємо, що сьогодні існує необхідність застосування поліпарадигмального підходу до дослідження інформаційної війни як одного з аспектів сучасної соціально-політичної дійсності.

РОЗДІЛ 2. ОСОБЛИВОСТІ ВЕДЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ВІЙН

2.1. Форми сучасних інформаційних війн

Інформація в наше століття відіграє ключову роль у функціонуванні громадських інститутів і в житті кожного громадянина. Для нормального функціонування єдиного інформаційного простору потрібна уніфікація інформаційних і телекомунікаційних технологій. Це дає можливість посилювати свою політичну, економічну і військову перевагу за рахунок лідерства в інформатизації держав з високим науково-технічним і промисловим потенціалом.

У XX столітті інформаційне протистояння набуло ще більш витончених форм і використовувало у своїх інтересах інноваційні розробки в сфері комунікації, соціальних технологій та науково-технічного прогресу. Найчастіше політична пропаганда приймала настільки агресивні і жорсткі форми, що нагадувала інформаційну війну проти свого ж народу. У Радянському Союзі технології інформаційного протистояння проти зовнішнього ворога, гітлерівської Німеччини застосовувалися в період Великої Вітчизняної Війни і потім зберегли свою актуальність під час «холодної війни» [49, с. 111].

У XXI столітті фахівці вже змогли ідентифікувати кілька як традиційних, так і сучасних різновидів інформаційних протидій, що мають форм інформаційних воїн:

– командно-управлінська, націлена на канали зв'язку між командуванням і виконавцями з метою руйнування системи управління;

– розвідувальна війна – збір важливої у військовому відношенні інформації (як напад) і захист власної; електронна війна, спрямована проти

засобів електронних комунікацій – радіозв'язку, радіолокаційних станцій, комп'ютерних мереж;

– психологічна війна – пропаганда, «промивання мізків»,

– інформаційна обробка населення, що включають підрив громадянського духу, деморалізація Збройних Сил, дезорієнтація командування і війна культур;

– хакерська війна, що передбачає диверсійні дії проти цивільних електронних об'єктів супротивника і захист від них (дії проти військових розцінюються як електронна війна), що може стати причиною серйозних та важких витрат – тотального паралічу різного роду мереж (електричних, електронних, комунікативних), введення випадкових помилок і комп'ютерних вірусів в пересилку даних, несанкціонованим підключенням до мереж і їх таємному моніторингу з метою шантажу;

– економічна інформаційна війна, що має дві форми – інформаційна блокада (перекриття каналів комерції та комунікації) й інформаційний імперіалізм (частина загальної політики економічного імперіалізму) [13, с.77].

Також до цього переліку належить кібервійна – відрізняється від «звичайного» хакерства, що передбачає захоплення комп'ютерних даних, що дозволяють відстежити супротивника (або шантажувати його) [14].

Припустімо, що подібного роду «комунікативні технології» поступово проникають з міжнародної політичної арени в бізнес-середовище. Натомість сучасний «дикий ринок» отримав нові ресурси, і, відповідно, будуть затребувані фахівці, які володіють цими технологіями.

Практика останніх збройних конфліктів демонструє, що одними з найважливіших механізмів війни стають не тільки зміни у військовій справі, але й інформаційна революція, яка зараз переживає стадію формування.

Початковий досвід ведення інформаційної боротьби в оперативному масштабі, як однією із складних військових протиборств, був заснований у війні в зоні Перської затоки у 1991 році. Успіх застосування інформаційної зброї не тільки окрилив США в розумінні ролі інформаційної боротьби, але надав приклад іншим державам, як її застосовувати та вести [19].

У серпні 1995 року Національним Інститутом Оборони США була опублікована робота Мартіна Лібікі – одного із провідних теоретиків у сфері інформаційних війн. У ній автор виділив 7 основних форм інформаційної війни[28]. Тож розглянемо їх докладніше.

Командно-управлінська форма інформаційної війни – спрямована на канали зв'язку між командуванням і підлеглими з метою позбавити останніх управління й координації зверху.

Розвідувальна – полягає в зборі та захисті військово значимої інформації.

Психологічна – інформаційна обробка населення – це своєрідне «промивання мізків».

Хакерська – передбачає певні дії, які призводять до збоїв в роботі зв'язку. Зброєю в даному виді війни виступають комп'ютерні віруси.

Економічна форма інформаційної війни визначається інформаційною блокадою й інформаційним імперіалізмом. Вчений Лібікі розглядає два види цієї війни – інформаційна блокада (направлення проти США) й інформаційний імперіалізм (метод самих США). Під блокадою розуміється, передусім, перекриття каналів комерції (за аналогією із забороною «фізичної» торгівлі). Злом банківської мережі в дану категорію не входить (це категорія хакерської війни). Інформаційний імперіалізм – частина загальної політики економічного імперіалізму.

Електронна – передбачає виведення з ладу електронних засобів зв'язку: комп'ютерних мереж, стільникових веж, радіовузлів тощо.

Кібервійна – форма інформаційної війни, котра, на відміну від хакерської війни, кінцевою метою має захоплення інформації [28].

Зауважимо, що наймасштабнішою і небезпечною здебільшого вважається психологічна війна. Вона справляє інформаційний вплив на широкі кола громадськості. Утім, для того, аби інформаційний вплив виявився ефективним, необхідна часткова присутність правди. Щоправда на цьому фоні можуть надходити й необхідні порції неправдивих даних.

Найбільш ефективний метод полягає в розчленуванні явища, виділення справжніх, але одиничних фактів й ототожнення їх із самим явищем, тобто створення на основі справжніх фактів помилкової інформаційної структури. Складні утворення такого роду носять назву політичних міфів. Упровадження у свідомість політичних міфів дозволяє замінити цілісний світогляд на фрагментарний, що викривляє реальну картину.

Грамотне поєднання таких міфів змінює ставлення суспільства до певної проблеми.

Основними формами ведення технічної інформаційної війни є радіоелектронна боротьба, війна з використанням засобів електронної розвідки і наведення, нанесення віддалених точкових ударів з повітря, психотропна війна, боротьба з хакерами, кібернетична війна [33].

Утім, перш ніж серйозно розбирати різні визначення інформаційної війни з технічної точки зору, зауважимо важливу їй властивість: ведення інформаційної війни ніколи не буває випадковим або відокремленим, а передбачає узгоджену діяльність з використання інформації як зброї для ведення бойових дій – чи то на реальному полі бою, або в економічній, політичній, соціальній сферах.

У цьому контексті основним і найбільш загальним визначенням інформаційної війни виступає наступне: «Інформаційна війна – це всеохоплююча цілісна стратегія, зумовлена все зростаючою значимістю й

цінністю інформації у питаннях командування, управління і політики» [37, 99].

Варто зауважити, що поле дії інформаційних воєн при такому визначенні виявляється досить широким і охоплює наступні області:

– інфраструктуру основних систем життєзабезпечення держави телекомунікаційні, транспортні мережі, електростанції, банківські системи тощо;

– промислове шпигунство – розкрадання патентованої інформації, перекручування чи знищення особливо важливих даних, послуг, збір інформації розвідувального характеру про конкурентів тощо;

– злам і використання особистих паролів VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, створення і продукування дезінформації;

– електронне втручання в процеси командування та управління військовими об'єктами і системами, «штабна війна», виведення з ладу мереж військових комунікацій;

– всесвітня комп'ютерна мережа Інтернет, у якій, за деякими оцінками, діють 150.000 військових комп'ютерів, і 95% військових ліній зв'язку проходять по відкритих телефонних лініях [42, с. 128].

Варто зазначити, який би сенс в поняття «інформаційна війна» не вкладався, воно народилося в середовищі військових і позначає, перш за все, жорстку, рішучу й головне – небезпечну діяльність, яку можна порівняти з реальними бойовими діями.

Військові експерти, сформулювали доктрину інформаційної війни, чітко уявляють собі окремі її грані: це штабна війна, електронна війна, психотропна війна, інформаційно-психологічна війна, кібернетична війна тощо.

Отже, інформаційна війна передбачає різні форми конфлікту, в якій відбуваються прямі атаки на інформаційні системи для впливу на знання або припущення противника. Інформаційна війна може проводитися як частина більшого і більш повного набору військових дій. Таким чином під загрозою інформаційної війни розуміється намір певних сил скористатися разючими можливостями, прихованими в комп'ютерах, на неозорому кіберпросторі, щоб вести «безконтактну» війну, в якій кількість жертв (у прямому значенні слова) зведено до мінімуму.

«Ми наближаємося до такого ступеня розвитку, коли вже ніхто не є солдатом, але все є учасниками бойових дій, – сказав один з керівників Пентагону. – Завдання тепер полягає не в знищенні живої сили, але в підриві цілей, поглядів і світогляду населення, в руйнуванні соціуму» [45].

Громадянська інформаційна війна може бути розв'язана терористами, наркотичними картелями, підпільними торговцями зброєю масового ураження. Військові завжди намагалися впливати на інформацію, яку потребував ворог для ефективного управління своїми силами. Зазвичай це робилося за допомогою маневрів і відволікаючих дій.

Оскільки ці стратегії впливали на інформацію, що отримує ворог, побічно шляхом сприйняття, вони й атакували інформацію ворога побічно. Тобто, для того, щоб хитрість була ефективною, ворог повинен був зробити три речі:

– спостерігати обманні дії;

– порахувати обман правдою;

– діяти після обману відповідно до цілей того, хто обманює [39, с. 92].

Проте, сучасні засоби виконання інформаційних функцій зробили інформацію вразливою до прямого доступу і маніпуляції з нею. Сучасні технології дозволяють противнику змінити або створити інформацію без

попереднього отримання фактів та їх інтерпретації. Ось короткий список характеристик сучасних інформаційних систем, що призводить до появи подібної уразливості: концентроване зберігання інформації, швидкість доступу, повсюдна передача інформації, і великі можливості інформаційних систем виконувати свої функції автономно. Механізми захисту можуть зменшити, але не до нуля цю уразливість.

Отже, інформація сьогодні є засобом ведення інформаційних воєн та ефективним інструментом досягнення суспільно-політичних цілей держави. Ведення інформаційного протистояння (передусім залежно від масштабів) може відбуватися в кількох формах, які ми проаналізували вище. Водночас зазначимо, що масштаб агресії або обрана мета не матимуть реального значення, якщо інформаційне протистояння дозволило досягти бажаного для певної держави наслідку.

2.2. Види інформаційних війн

Інформація, яка визначається як сигнали або відомості, сприйняті приймачем та перетворені у сигнали керування, сьогодні активно використовується як ефективний інструмент досягнення суспільно-політичних, економічних, геополітичних цілей держави, а за допомогою сучасних інформаційних технологій перетворена на потужну зброю масового ураження. Адже боротьба держав в інформаційному просторі ведеться за зони політичного й економічного впливу, джерела сировини, ринки збуту й території, а всередині країни – за владу, власність, політичний вплив, можливість маніпулювати настроями й поведінкою громадян

Зазначене призвело до появи й активного ведення інформаційних війн нового покоління – проведення широкомасштабних інформаційних дій, що застосовуються сторонами, які знаходяться у протиборстві [5, с.173]. Вони

стали несиловим засобом забезпечення державами власних інтересів та вирішальним фактором в досягненні результатів.

Якщо розглядати ***види інформаційних війн (***Рис 2.1.***)***, то вони поділяють на наступні категорії:

1*) За учасниками*:

– на комерційні, що відбуваються між організаціями і підприємствами;

– міждержавні, що відбуваються між державами і державними союзами;

– та політичні, які, в свою чергу здійснюються між політичними діячами та партіями.

2) За методами ведення:

- війна першого покоління;
- війна другого покоління;
- війна третього покоління;
- війна четвертого покоління.

Рис. 2.1. Види інформаційних війн

Відповідно до класифікації, інформаційні війни є війнами сьомого покоління. Їх поява стала наслідком наступних чинників:

– розвиток засобів обчислювальної техніки і комунікації [2];

– розвиток прикладної психології у сфері вивчення поведінки людей та управління їх мотиваціями [5];

– глобалізація та масштабна інформатизація суспільства.

– Серед багатьох їх різновидів під час ведення інформаційної війни ключовим є інформаційний [9], над ефективність якого забезпечують:

– активне впровадження у фахову діяльність і повсякденне життя людей електронних інфо-комунікаційних систем, соціальних мереж, мобільних пристроїв тощо;

– інтеграція у життя й виникнення стійкої залежності сучасної людини від інформаційно-телекомунікаціних, мережевих, мобільних засобів

тощо, які стають основним джерелом інформації, а, отже, формують думку, світогляд та поведінку громадськості.

Ефективність інформаційних впливів під час ведення інформаційних війн визначається передусім умінням використовувати саму інформацію. Складана когнітивно-аксіологічна природа інформації штовхає до пошуку новітніх тактичних та стратегічних прийомів для здійснення інформаційних впливів, які допоможуть досягти бажаних завдань та мети [15, с. 70].

За інтенсивністю, масштабами та засобами, що використовуються, можна вирізнити такі види інформаційного протиборства: інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою поступової, планової, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії:

– витіснення положень національної ідеології та національної системи цінносте і заміщення їх власними цінностями та ідеологічними настановами;

– збільшення ступеня свого впливу та присутності, введення контролю над стратегічними інформаційними ресурсами;

– інформаційно-телекомунікаційною структурою і національними ЗМІ;

– нарощування присутності власних ЗМІ в інформаційній сфері об’єкта проникнення тощо.

Інформаційна агресія – дії, спрямовані на завдавання супротивникові конкретного, відчутного збитку в окремих сферах його діяльності. Вирізняють такі ознаки інформаційної агресії:

– обмежене й локальне за своїми масштабами застосування сили;

– контрольоване, дозоване завдавання шкоди;

– вилучення із засобів інформаційного впливу найнебезпечніших видів, що не дають змоги надійно контролювати розміри шкоди – інформаційної зброї;

– обмеження розмірів простору, кількості об’єктів, інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційним впливом (агресія зачіпає не весь інформаційно-психологічний простір держави-жертви, а тільки його частину), обмеження цілей і час (зазвичай агресія припиняється після цілковитого досягнення агресором усіх поставлених конкретних намірів і зрідка набуває затяжного характеру), а також за залученими силами і засобами;

– природна релаксація ефекту від агресивного інформаційного впливу після припинення активності джерела агресії [18].

Можемо погодитися із науковцем Г. Почепцовим, котрий інформаційну війну визначає як комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив обох сторін одна на іншу, що охоплює систему методів та засобів впливу на людей, їхню психіку, поведінку тощо [44].

З огляду на це проаналізуємо окремі види інформаційної війни.

1. Кібервійна як інформаційне протиборство в кіберпросторі. Проаналізуємо цілі кібервійни: дестабілізація комп'ютерних систем, порушення доступу до Інтернету державних установ і ділових центрів, створення безладу і хаосу в житті країн.

Форми прояву кібервійни:

– вандалізм;

– пропаганда;

– шпигунство;

– атаки на комп'ютерні системи і сервери.

2. *Мережеві війни і їх особливості*.

Мережева війна (Netwar) – ширший феномен, пов'язаний з особливостями і викликами інформаційної ери та глобалізації. Цей інструмент використовується не тільки у традиційній військовій сфері, а й для впливу на широкі верстви населення на когнітивному рівні [6].Головна мета інформаційно-мережевої війни – «це захоплення території, встановлення над нею контролю без використання класичної зброї і, якщо це можливо, без прямої воєнної агресії».

3. Концепція Мережецентричної війни – мережецентричні бойові дії (Net-Centric Warfare) – це суто військова концепція, що пройшла тривалий шлях від інтелектуальних розробок і мозкових штурмів через експерименти до практичних дій, які вплинули на зміну інфраструктури Пентагону і військову стратегію США [39, с. 173].

Інформаційно-мережеві війни здебільшого відбуваються без використання класичних засобів озброєння. Ці конфлікти є логічним наслідком геополітики і ніколи не ведуться прямо. Для початку мережевої операції потрібно створити умови, за яких сторони протиборства будуть зацікавлені в реалізації певного сценарію. При цьому немає єдиного центру ухвалення рішень, а лише певний контекст (намір командира), який підхоплюють та інтерпретують учасники мережі.

Немає прямих команд, є певні очікування, що озвучують представники центру мережевих операцій (мозкового центру вироблення концептуальних рішень). Виконавці отримують тільки загальне уявлення про завдання, а головне – їм надають можливість самостійно шукати шляхи найефективнішого його розв'язання залежно від конкретних умов.

Припустімо, що хтось уміщує в ЗМІ інформацію, яка згодом поширюється мережею, а її учасники вже сприймають відомості як керівництво до дії, виходячи з обставин і, що важливо, самостійно приймають рішення.

Водночас, спостерігається стрімке вдосконалення засобів ведення інформаційної боротьби. Першочергово це стосується інформаційної зброї, яка призначена для боротьби з комп'ютерними мережами і системами управління. До сучасної інформаційної зброї входить сукупність спеціально організованої інформації та інформаційних технологій, що дозволяє цілеспрямовано змінювати, знешкоджувати, копіювати, блокувати інформацію, долати системи захисту, здійснювати дезінформацію, пошкоджувати функціонування носіїв інформації, інфокомунікаційних систем та мереж [18].

Отже, з означеного випливає, що актуальною задачею є постійний моніторинг відповідними органами держави проявів ознак інформаційної експансії, агресії, війни [46] або їх гібридів, яку слід сприймати як пряму загрозу національній безпеці та невідкладно вживати належних заходів і застосування засобів інформаційної протидії й захисту.

Таким чином, метою роботи є розроблення моделі адекватної поведінки держави (її відповідних органів) на ранніх стадіях інформаційної експансії, агресії, війни або їх гібридних форм.

Слід зазначити, що наразі сучасні науковці акцентують увагу на інформаційно-комунікативній революції, яка відбувається у різних сферах. Виявом такої революції є перетворення акторів соціокультурного процесу на впливових авторитетних суб'єктів політики, яких готові підтримувати великі чи малі групи людей.

Окрім внутрішніх інформаційних потоків, значний вплив на свідомість і поведінку здійснюють зовнішні суб'єкти, які також мають авторитетні і широкі кола підтримки своїх дій і рішень, надаючи зразки ефективних моделей і технологій інформаційно-комунікативного характеру.

Інформаційна система має ознаки транснаціонального феномену, що не обмежується територіальними кордонами та розширює наші уявлення про

функціонування різних сфер суспільства. Це значно полегшує та прискорює засвоєння кращого зарубіжного досвіду, наприклад стосовно принципів і стандартів функціонування європейського освітнього простору [11].

Такі інформаційні впливи та інформаційні технології можуть спрямовуватися на вирішення поточних внутрішніх питань та інтеграцію національної системи освіти у світовий освітній простір. Це – важливе завдання в контексті реалізації євро інтеграційних стратегій України.

Для сучасної України велике значення має аналіз досвіду провідних країн світу щодо розвитку інформаційного простору та впливу інформаційної політики на процеси взаємодії між державними інститутами, громадськими об'єднаннями, усіма суб'єктами освітньої діяльності та зацікавленими в її результатах. Подібна зацікавленість притаманна практично усьому суспільству, яке користується продуктом освітньої сфери у вигляді підготовлених фахівців різного профілю, розроблених технологій, сформульованих стратегій розвитку чи окреслених моделей і тактики вирішення суспільно-значущих завдань.

Отже, в умовах нестримної світової глобалізації соціально-економічна, політична і культурна мережі пронизані інформаційними каналами й утворюють інформаційно-мережеві структури. Це дає можливість вести інформаційні війни на новому рівні, що зачіпає, окрім збройних сил, усю сферу соціуму: дипломатичні канали, інформаційну, соціально-культурну, світоглядну, фінансово-економічну, політичну й технологічну сфери, а також науку, психологію і внутрішній світ людини.

2.3. Методи і способи ведення інформаційних війн

Сучасні глобалізаційні процеси призвели до створення єдиного світового інформаційного простору, в якому інформація народжується, змінюється, зберігається й обмінюється між суб'єктами – людьми, організаціями, державами. Називаючи сучасне суспільство з його інформаційної надмірністю «цивілізацією шуму» [10, с.79], деякі дослідники порівнюють інформацію з надмірною радіацією, від якої неможливо сховатися, вказують на її особливу вірулентність.

Інформація онтологічна в тому сенсі, що пронизує всі сфери життєдіяльності соціального світу, є основою, на якій формується єдина картина світу. Інформаційна складова присутня як у фізичному світі у вигляді енергетичних або структурних характеристик об'єктів, так і в соціальній реальності, де вона існує в вигляді знань.

Нинішня цивілізація, що прискорює інформаційні потоки, трансформує глибинні структури інформації, призводить до появи інфосфери, в якій людина концентрує і переробляє інформацію, відповідно до своєї інформаційно-комунікативної компетентності. При цьому сучасна культура актуалізує спілкування людини не з реальністю як такої, а її репрезентацією. Поведінка людини зумовлюється не відображенням об'єктивної реальності, а суб'єктивними уявленнями про «реальності для суб'єкта».

Відбувається своєрідна заміна реальних об'єктів віртуальними, подобами, що «симулюють» соціальні відносини і культурні феномени. Наступила «ера невагомості», що не вимагає критичного мислення і сприяє маніпулюванню свідомістю і передбачає пасивність як кінцеву його мету [27, с. 143].

Сформована в індивідуальній і суспільній свідомості реальність схильна до зовнішнього впливу. Особливістю впливу на інформаційні потоки сьогодні є те, що воно здійснюється цілеспрямовано. Сформований інформаційний простір стає ареною інформаційного протиборства, де метою є знання, свідомість (від лат. «*conscientia*») суб'єкта, що підтверджує адекватність застосування концепції консціентальної війни при аналізі війни інформаційної.

Консціентальна війна – війна психологічна за формою, цивілізаційна по змісту та інформаційна за засобами, в якій об'єктом руйнування і перетворення є свідомість і ціннісні установки населення противника [34]. Очевидність зв'язку ціннісних установок людини з культурою його народу вказує на той факт, що об'єктом руйнування в консціентальній війні є духовна єдність нації, культурна оболонка супротивника, культурна ідентичність.

Консціентальна війна пов'язана із захопленням, зломом і зміною свідомості об'єкта агресії. Вона має форму зсуву ціннісних орієнтирів, а закінчується поразкою свідомості противника, знищенням його здатності до самоідентифікації та самовизначення, підбиттям до прийняття реальності нового буття, а в підсумку – приведенням країни в стан дезорієнтації.

Консціентальна зброя:

– вражає і руйнує свідомість шляхом дезінтеграції і примітивізації інформаційно-комунікативного середовища, в якій «живе» свідомість;

– поширення по різних телекомунікаційних каналах, порушують роботу останнього;

– руйнування способів і форм ідентифікації, що призводить до втрати ідентичності, а також знищення системи цінностей, замінних з подальшим культурним перевербуванням;

– позбавлення противника здатності ставити глобальні й стратегічні цілі тощо.

«Екранна» культура стає новим театром військових дій у цій психологічній війні. Демонстроване на телевізійному екрані являє собою особливий «ангажований» дискурс, який оперує інформаційно-віртуальними об'єктами, а тому не тільки сама інформація, а й її обговорення, реакція на неї належать тому, хто «спостерігає».

Таким чином, інформаційна війна є «найбільш інтелектуальним варіантом військового протиборства, оскільки і суб'єкт, і об'єкт впливу тут є людським розумом. Якщо звичайна війна націлена на тіло людини, то інформаційна або смислова – на його розум» [21, с.62].

Інформаційний компонент соціо-системи надзвичайно вразливий і важливий, оскільки інформація – це не тільки «передане», а й те, що представляє «інформаційне ядро» будь-якої системи, то, що змінює індивідуальне і масову свідомість, призводить до зміни останньої або її трансформації. Саме тому в постіндустріальному медійному світі держави зацікавлені в створенні і захисті вигідного для себе інформаційного середовища.

Інформаційна війна, по суті, тотальна в тому сенсі, що дійсно є війною не армії та військових, а націй, вимагає мобілізації всіх ресурсів держави, і ведеться в глобальному інформаційному просторі. використовуючи найбільш руйнівні види зброї – слово й інформацію.

Крім того, інформаційна війна універсальна, оскільки, по-перше, вона може вестись у всіх сферах суспільного життя – економічній, політичній, соціальній, військовій, духовній.

По-друге, вона самодостатня і може як обходитися без традиційних засобів і способів збройної боротьби, так і поєднувати їх з іншими видами бойових дій. Інформаційна війна має чітку структуру. Вона розгортається в

інформаційному просторі – просторі епістемологічного, психолого-смислового, в якому інформаційні технології породжують, передають і зберігають смисли, що володіють потенціалом, що здатен трансформувати дійсність. З розвитком інформаційної цивілізації вони стають основними продуктивними силами, що створюють інформацію та знання, тобто ті смисли, які і є об'єктами агресії в інформаційній війні, одночасно представляючи і «найбільшу небезпеку як нового знаряддя атаки» [41].

За спрямованістю інформаційних впливів можливе виділення двох основних типів інформаційної війни:

– інформаційно-психологічного;

– інформаційно-технічного з використанням відповідного виду зброї [22, с. 96].

Засоби зазначених видів інформаційної війни передбачають організацію двох груп заходів. Перша пов'язана з консціентальним характером інформаційної війни і має на меті вплив на системи формування громадської думки і прийняття управлінських рішень, а також свідомість військовослужбовців і цивільне населення для його «перепрограмування».

Друга – орієнтована на поразку інформації та інформаційно керуючих систем противника. Засоби, що використовуються при реалізації цих заходів різноманітні: психологічні операції з метою впливу на політичне та військове керівництво, військовослужбовців, а також цивільне населення противника; дезінформація тощо.

Успішність ведення інформаційної війни залежить від досягнення трьох основних цілей:

– контролю інформаційного простору і забезпечення захисту власної інформації;

– забезпечення наступальних інформаційних дій;

– оптимізації загальної ефективності дій збройних сил [8, с. 130].

У суб'єктної складової цієї структури можливе виділення якогось Центру – органу управління інформаційною війною; агентів впливу, перетворюючих стратегію і тактику інформаційної війни в життя; зацікавлених осіб («господарів дискурсу»), що несуть в залежно від ведення або припинення інформаційної війни вигоди або збитки.

Методи інформаційної війни надзвичайно різноманітні:

– дезінформація,
– пропаганда,
– наклеп,
– брехня,
– приховування суттєвої інформації,
– зміщення понять,
– відволікання уваги,
– інформаційне табу тощо.

В інформаційному світі людина, суспільство і держава можуть розглядатися як інформаційні самоосвітні системи [18], і завдання противника – ефективне перепрограмування, перекодування останніх з попередніми приведенням їх у стан хаосу шляхом руйнування їх «ядерної» інформації. Тому основною проблемою інформаційної війни стає захист знання. Людина, суспільство, держава стають учасниками інформаційних воєн, що пов'язане з погрозами, збитками, ризиками. Від їх нейтралізації (або хоча б мінімізації) залежить перемога або поразка.

Еволюція методів ведення інформаційної війни свідчить про зміну поколінь інформаційного протиборства: від першого покоління, більш орієнтованого на дезінтеграцію систем управління і проведеного як забезпечення дій традиційних сил і засобів, до стратегічного інформаційного

протиборства другого покоління, заснованому на скоординованих інформаційних операціях, які приводять у результаті до неможливості застосування сили [22, с. 106]. Але сьогодні операції на основі ефектів – «швидких вирішальних дій» – представляють собою третє покоління методів інформаційної війни. Вони розроблені як об'єднуючі передові концепції високоточного удару, домінуючий маневр і інформаційні операції по всьому бойовому простору, даючи можливість створити ефекти і викликати зміни в поведінці противника.

Їх основою стає мережеве протиборство, яке включає одночасні дії в фізичному, інформаційному і «психолого», епістемологічному просторі противника. Це нова філософія війни, що дає можливість отримати бажаний стратегічний результат («ефект») через застосування повного діапазону військових і невійськових заходів на тактичному, оперативному і стратегічному рівнях.

Оскільки результатами інформаційної війни стають створення атмосфери бездуховності, аморальності, політичної нестабільності, економічного хаосу, приведення країни противника в некероване і стан дезорієнтації, остільки нинішнє інформаційної війни вимагає не тільки осмислення нового досвіду, а й генерування нових теорій, спрямованих на захист власного інформаційного простору.

Інтелектуальна, смислова природа інформаційної війни буде сприяти збільшенню «кількості критичних областей, в яких буде спостерігатися перевищення необхідності швидкості прийняття рішень над гранично можливою швидкістю реакції людини» [10].

Отже, будуть рости і руйнівні можливості інформаційних воєн, а також вимоги до забезпечення інформаційної безпеки держави, підвищення компетентності фахівців інформаційної боротьби в сфері інформаційно-

технічної війни, а також захисту свідомості громадян держави, що є пріоритетним при веденні інформаційно-психологічного протиборства.

РОЗДІЛ 3. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

3.1. Виклики і загрози безпеці України в інформаційній сфері

Сьогодні, коли відбуваються сучасні глобальні та регіональні інформаційні протистояння, створюються деструктивних комунікативні впливи, сутички різновекторних національних інформаційних інтересів, дедалі більше поширюється інформаційна експансія та агресія, стратегічними завданнями країн в системі глобальних відносин постають захист національного інформаційного простору та гарантування інформаційної безпеки. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері набувають особливого, пріоритетного значення для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та деструктивного інформаційного вторгнення [26, с. 57].

Сьогодні в умовах російсько-українського конфлікту наша держава нагально потребує захисту національного інформаційного простору від негативних інформаційно-психологічних впливів та війн, а також гарантування інформаційної безпеки та інформаційного суверенітету своїм громадянам. Подолання зазначених загроз стає важливим фактором збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

Інформаційна безпека є інтегрованою складовою національної безпеки і її досліджують як одну із пріоритетних позицій держави. Інформаційна безпеки, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності

суспільства, збереження інформаційного суверенітету, протидію негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій.

Вирішення проблеми інформаційних загроз країні дасть змогу забезпечити захист інтересів суспільства і держави, гарантуватиме право громадян на отримання якісної та об'єктивної інформації.

Проблему інформаційної безпеки у контексті національної ми можемо трактувати з точки зору двох аспектів. По-перше, інформаційна безпека розглядається як самостійний елемент загальнонаціональної безпеки будь-якої держави, а по-друге – як інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо.

Проблема гарантування інформаційної безпеки України актуалізується в умовах війни на Сході, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіа заходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість [45, с. 371].

Наразі можемо констатувати, що в Україні через посилення негативного зовнішнього впливу на інформаційний простір виникають загрози поступового цілеспрямованого знищення суспільних цінностей, національної ідентичності. При цьому відзначимо недостатніми залишаються обсяги створення національного конкурентоспроможного інформаційного продукту. Крім того, критичним можна назвати стан безпеки інформаційно-комп'ютерних систем у сфері державного управління, фінансової та

банківської сфер, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Нинішні воєнно-політичні умови в яких існує вже упродовж 5 років існує Україна обумовлює необхідність суттєвого корегування низки аспектів державної політики, і передусім – інформаційної та правової. П'ять років агресії, у тому числі й інформаційної, зумовили пошук державою та її громадянами механізмів протидії деструктивній російській пропаганді, а сама інформаційна агресія «оголила» системні проблеми української держави в сфері захисту свого інформаційного простору від ворожих дій супротивника.

Водночас у сфері безпосереднього відбиття інформаційної агресії за період з 2014 по 2020 роки було віднайдено цілу низку вагомих рішень, починаючи від системного пошуку фейків у повідомленнях російських ЗМІ, і закінчуючи активними інформаційними контрзаходами. Власне саме ці фактори, що здебільшого реалізуються не державними гравцями (як неурядовими організаціями, так і окремими неформалізованими групами), кидають своєрідний виклик традиційній державній політиці (або державним практикам реалізації державної політики). Саме вони і породжують цілий спектр того, що можна назвати «сірими рішеннями».

З огляду на це, зазначимо, що саме недержавні гравці мають низку переваг, що вигідно вирізняє їх у питаннях відбиття інформаційної агресії від офіційних державних структур. Мається на увазі їхні здатність оперативно діяти, мінімізуючи при цьому бюрократичні процедури; чинити публічно в умовах відсутності достатніх даних для такої діяльності; оперативно залучати необхідні ресурси й піддатливо реагувати на зміни в інформаційному середовищі [52].

Утім необхідно визнати, що багато в чому діяльність недержавних структур є саме тим, що хотіла б робити держава, однак не може через

чимало об'єктивних обставин. Зокрема, держава обмежена у своїй діяльності національним та міжнародним законодавством, а також уявленнями наших західних партнерів щодо того, як має себе поводити «відповідальна демократична та правова держава». Проблема в тому, що більшість з цих норм мало застосовуються в умовах гібридного конфлікту та масштабної інформаційної війни, яка ведеться в Україні і проти України. І власне саме тому дії недержавного сектору це часто те, що має бути зроблено, однак не завжди – те що законно. Адже подекуди діяльність цих «недержавних акторів» породжує неоднозначну дилему щодо цілісності/фрагментарності правового поля держав.

Можливі інформаційні загрози для нашої країни узагальнено у кількох чинних нормативно-правових актах, таких як Закон України «Про основи національної безпеки України» [1], указах Президента України «Про затвердження Доктрини інформаційної безпеки України» та «Про Стратегію національної безпеки» [4]. На відомчому рівні інформаційні загрози для нашої держави узагальнено у Концепції забезпечення інформаційної безпеки Міноборони та Збройних Сил України [3].

У цих державних документах також визначено сфери життєдіяльності суспільства й держави, вразливих до інформаційних загроз, зокрема це: зовнішньополітична, внутрішньополітична і воєнна сфери, економічна, соціальна, гуманітарна, науково-технологічна й екологічна галузі, державна безпека.

Зазвичай, серед найбільш небезпечних загроз ми вважаємо ті, що мають вплив на воєнну сферу.

Відповідно до нормативно-правових актів, зазначених вище, а також ураховуючи практичний досвід роботи щодо вияву та аналізу інформаційних загроз, основними небезпеками, що становлять загрозу державі в інформаційній сфері є:

1) використання інформаційного простору для підготовки та здійснення збройної агресії проти держави, перспектива втягнення її у збройні конфлікти чи військові протистояння з іншими державами шляхом використання інформаційного простору;

2) порушення законодавства стосовно збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу держави;

3) несанкціонований доступ до інформаційних і телекомунікаційних систем та мереж загальнонаціонального значення, що може порушити діяльність військових формувань, органів військового управління, ЗС України в цілому, або втручання в автоматизовані системи керування зброєю;

4) реалізація програмно-математичних заходів та застосування інформаційних технологій з метою порушення функціонування систем управління воєнної сфери та сфери оборони;

5) реалізація інформаційного впливу на населення країни з метою дискредитації воєнно-політичного керівництва держави, підбурювання людей до перешкоджання функціонування й діяльності військових частин (організацій, установ, підприємств), погіршення іміджу військової служби;

6) здійснення інформаційного впливу на особовий склад військових частин та підрозділів з метою дискредитації та втрати довіри до військового командування, зниження рівня морально-психологічного стану та готовності військовослужбовців до оборони держави;

7) активне зміцнення потенціалу більшості країн світу в сфері оборони в напрямку посилення можливостей ведення дій в інформаційному просторі та захисту від аналогічних дій з боку супротивника;

8) порушення встановлених норм і вимог із протидії технічним розвідкам щодо військових об'єктів, зразків озброєння, військової та спеціальної техніки;

9) будь-яка діяльність, здійснена зловмисно, а також помилки працівників підчас роботи в інформаційних та інформаційно-телекомунікаційних системах;

10) відсутність достатньої кількості портативних захищених засобів зв'язку та їх несумісність із засобами зв'язку інших військових формувань України;

11) проблеми соціального захисту військовослужбовців та членів їх сімей, які залишаються невирішеними [45].

Вважаємо за доцільне виділити інформаційні загрози щодо воєнної сфери, які виникли у зв'язку із веденням гібридної війни проти України:

1) поширення недостовірної, перекрученої та упередженої інформації (дезінформації), що дискредитує військове керівництво, ЗС України, Операцію об'єднаних сил (ООС) (антитерористичну операцію (АТО));

2) розповсюдження інформації, спрямованої на деморалізацію особового складу силових структур, задіяних в ООС (АТО), та звинувачення їх у причетності до незаконних дій у зоні конфлікту: мародерстві, продажу зброї і техніки, контрабанді тощо);

3) поширення інформації, яка дискредитує конкретні військові формування, військову службу та військовий обов'язок, провокує зрив мобілізації в країні;

4) розповсюдження дезінформації іноземними ЗМІ щодо недопущення надання військової допомоги Україні прихильними до неї країнами. До речі, слід зазначити, що за останні роки присутність Росії в інформаційному просторі України значно зросло і для того, аби подолати ці загрози

національній інформаційній безпеці треба ліквідувати джерела інформації, котрі працюють проти України. Помітно, що інформаційний вплив сусідньої держави достатньо потужний і за останні роки лише зростає. Навіть 5 років тому присутність Росії в українському інформаційному просторі не було таким яскравим як сьогодні.

Проти України прямо працюють кілька каналів. І не тільки радійних або телевізійних. В Україні відсутні дієві інститути по забезпеченню інформаційної безпеки країни.

Зауважимо, що у Воєнній доктрині України йдеться про те, що планомірний інформаційний або інформаційно-психологічний вплив із застосуванням нових інформаційних технологій вважається серйозним воєнно-політичним викликом, який може перетворитися на загрозу війни [2].

Згідно із Законом України «Про основи національної безпеки» будь-які спроби маніпулювання свідомістю, зокрема, шляхом поширення дезінформації, становлять воєнну загрозу національним інтересам країни в інформаційний сфері [1].

Відповідно до Доктрини інформаційної безпеки України здійснення спеціальних операцій з дезінформації, спрямованих на підривання обороноздатності країни, деморалізацію особового складу ЗСУ, проведення державою-агресором спеціальних операцій з дезінформації в інших країнах з метою створення негативного іміджу України у світі, інформаційне домінування країни-агресора на тимчасово окупованих територіях вважається воєнними загрозами національним інтересам в інформаційний сфері [19].

Крім того, Концепція розвитку сектору безпеки і оборони України визначає, що цілеспрямований інформаційний та інформаційно-психологічний вплив на формування негативного міжнародного іміджу України, дестабілізацію внутрішньої суспільно-політичної

ситуації, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин є безпековим викликом, що може посилювати воєнну загрозу [45].

Наведемо приклад, Досить важливим внутрішнім фактором є «розірвана на шматки» духовність українського суспільства. Індійський філософ Ш.А. Грош зазначав: «Духовність у своїй суті є пробудженням внутрішньої дійсності нашого створіння, нашої душі, внутрішнє прагнення пізнати, відчути і ототожнити себе з нею, увійти в контакт з вищою дійсністю, об'єднатися з нею, і як наслідок – перетворити все наше єство на нову особистість, нову природу» [22].

Серед зазначеного переліку ми вбачаємо внутрішні та зовнішні загрози. Деякі з них можуть прямо впливати на національну безпеку держави, а деякі – опосередковано. Частина зовнішніх загроз реалізується безпосередньо, а частина має форму потенційних загроз, викликів або ризиків.

Згідно зі Стратегією національної безпеки України інформаційно-психологічна війна, приниження української мови і культури, фальшування історії, формування російськими засобами масової комунікації альтернативної дійсності викривленої інформаційної картини світу вважається актуальною загрозою національній безпеці України в інформаційній сфері [4].

Ці виклики, ризики та загрози за своєю природою є інформаційними. Утім реалізація їх може спричинити суттєві, і навіть дуже важкі та критичні наслідки у воєнній сфері. Наразі ефективно реалізуються інформаційні загрози, які здійснюються засобами інформаційного впливу на населення державою-агресором для дискредитації політичного керівництва «держави-жертви», підбурювання громадян для дестабілізації внутрішньої суспільно-політичної ситуації, загострення міжетнічних та міжконфесійних взаємин,

для деморалізації населення, зниження рівня його морально-психологічного стану та готовності до збройної боротьби.

Приміром, під час війни в Іраку у 1991 році комплексний надпотужний інформаційно-психологічний вплив на особовий склад армії Іраку, який був організований багатонаціональними силами, сприяв виконанню бойових завдань із мінімальними втратами військових та техніки. При цьому тривалий час різноманітні засоби впливу (листівки, теле- і радіотрансляції з борту спеціальних літаків сил психологічних операцій) всіляко перебільшували «необмежені можливості» американської бойової техніки і залякували іракських військових її вражаючими потужностями. В результаті, більшість військових ще на початку бойових дій одразу почали здаватися у полон [25].

Серед сучасних прикладів, що яскраво ілюструють інформаційні загрози, які трансформувалися у воєнні дії, є дії Російської Федерації щодо анексії Криму у ході гібридної війни проти України, підготовку до якої російське керівництво розпочало задовго до активних силових дій. На підтвердження завчасних агресивних планів Кремля доцільно згадати твердження начальника Генерального штабу ЗС РФ генерала армії В. Герасимова, зроблені ним за рік до початку анексії Криму. Він у своїй доповіді стосовно тенденцій розвитку й удосконалення форм і способів застосування збройних сил, на науковій конференції Академії військових наук РФ ще у 2012 році наголошував, що «… у війнах XXI століття акцент змістився на використання політичних, економічних, інформаційних, гуманітарних та інших невоєнних заходів поряд із використанням протестного потенціалу місцевого населення. Все це повинно супроводжуватися прихованими військовими операціями – наприклад, методами інформаційної війни і використанням спецназу...» [45, с. 291].

Крім того, під дією дуже потужного інформаційно-психологічного впливу на особовий склад підрозділів і частин Збройних Сил, які до початку російської агресії базувалися в Криму, а також на їхні сім'ї, Кремлю вдалося деморалізувати значну частину українських військових, змусити їх зрадити присязі й залишити військові частини. Це призвело до часткової або повної втрати бойової готовності окремих частин і підрозділів. Результатом стало захоплення російськими військами цілих військових містечок на території Криму [18]. Це свідчить про надзвичайно важливу роль тих інформаційних загроз, які весь інформаційний й психологічний вплив, спрямували на дестабілізацію соціально-політичної ситуації в країні.

Тоді упродовж підготовчої фази гібридної війни Росія здійснювала всебічні заходи впливу на українське керівництво для того, щоб змусити його погодитись на умови Кремля, змінити зовнішньополітичний курс країни на проросійський й надалі узгоджувати з РФ національну зовнішню і внутрішню політику.

Тоді заздалегідь за кілька років розпочалось проведення тривалих потужних антиукраїнських інформаційних операцій. Їхнім завданням було:

1) здійснити розкол українського суспільства та створити сприятливе підґрунтя для реалізації подальших планів Кремля;

2) об'єднати російське суспільство ідеями великодержавності та експансіонізму;

3) виправдати свої дії щодо України перед світовою спільнотою, нав'язуючи їй кремлівське бачення подій як виключно вірних [28].

Для упровадження антиукраїнської пропаганди керівництво Росії задіяло значні людські, матеріальні та потужні фінансові ресурси, завдяки чому вдалося ефективно «промити мізки» не лише більшості своїх громадян, а й значній частині українців. Тому, на жаль, це призвело

навесні 2014 року до підтримки частиною українських громадян агресивної політики Кремля проти України. Багато наших співвітчизників на сході країни під впливом російської пропаганди щиро вірили, що в Києві до влади прийшли фашисти й бандерівці, які «будують концентраційні табори і просто на вулицях вбивають за російську мову». Тому нову українську владу, силові структури країни, разом з українською армією, слід вважати ворогами.

Зазначимо, що в результаті цілеспрямованої роботи російської сторони на сьогоднішній день в кабельних мережах України здійснюють ретрансляцію «Перший канал», «НТВ-мир» та інші. «Перший канал» має пріоритет на російському ТБ в поширенні критичних висловлювань і сюжетів на адресу української державності, офіційної мови, громадян України. Так, в художніх фільмах російського виробництва, які демонструються на російських і українських каналах ТБ, українці представлені в негативному образі. Так, у фільмі «Брат 2» персонажі неодноразово називають українців «хохлами», висловлюють на їхню адресу зневажливі образливі вирази. У фільмі «Матч» негативні герої чомусь розмовляють українською мовою та носять жовто-блакитні пов'язки. Подібна концепція поширення комплексу неповноцінності українців чітко проглядається в російському кінематографі і є одним з типів сірої пропаганди.

Цілеспрямовані інформаційно-психологічні операції антиукраїнського змісту реалізуються шляхом розробки, виробництва і поширення негативних інформаційно-психологічних впливів. Застосовуються спеціальні засоби і методи такого впливу, здатні заблокувати на підсвідомому рівні свободу волевиявлення спільнот.

Так, вплив на широку аудиторію успішно здійснюється за допомогою розважальної індустрії. Продукція кінематографа блокує здатність аналізувати та логічно мислити, яскраво і емоційно передає інформацію, яка

легко засвоюється. Наступним за значенням засобом впливу на широкі маси населення в державі з боку РФ є преса, зокрема газети. Сьогодні в Україні видаються загальнонаціональні українські версії російських видань – «Комсомольська правда», «Коммерсант», «Известия», «Аргументи і факти» та інших. Цей фактор використовується в повній мірі, адже в інформаційній війні аналітичний чи розважальний матеріал може впливати на аудиторію не менше, ніж пряма політична реклама. При цьому російський капітал входить не тільки в сферу телерадіомовлення та друкованих ЗМІ, а й в сегмент роздрібного продажу преси, де створюються умови для витіснення вітчизняної періодики на користь російських і проросійських видань.

Таким чином, значна частина зовнішніх інформаційних загроз фактично є різновидом воєнних загроз і саме вони найнебезпечніші для системи забезпечення воєнної безпеки держави. Такі загрози починають реалізовуватися в інформаційній сфері і через інформаційну сферу, а завершують свою дію, завдаючи збитків важливим об'єктам воєнної сфери держави. Тобто, це загрози непрямої дії, їх важко виявити у воєнній сфері та своєчасно прийняти відповідні заходи протидії. Такі інформаційні загрози повинні виявлятися в інформаційній сфері ще на початковій стадії формування їх ознак та нейтралізуватися спільними зусиллями підсистем забезпечення інформаційної та воєнної безпеки системи забезпечення воєнної безпеки держави.

3.2. Механізми забезпечення інформаційної безпеки України

Дехто з науковців сьогодні відзначає, що на жаль, українська влада та українське суспільство ще не спромоглися належно протидіяти інформаційній експансії ворога, направленій на деконсолідацію українського

суспільства, що й призвело до настання нинішньої політичної ситуації в Україні.

Духовною є будь-яка діяльність, яка веде людину вперед у напрямку якоїсь форми розвитку: емоційного, інтуїтивного, соціального – і вказує на потужність і міць її життєвої внутрішньої сили.

Наразі в країні зі станом духовності значні проблеми. Глибоке соціальне розшарування суспільства, практична відсутність прошарку середнього класу, конфесійні конфлікти (серед яких розмежування Українська православної церкви Московського і київського патріархатів) фактично відкрито демонструють підтримку агресора нашої держави. Водночас її члени благословляли агресорів на вбивство українців і самі брали участь у цьому, про що свідчать наявні об'єктивні факти. Все це викликало велику політичну та соціальну напругу у суспільстві, що не сприяє руху України та побудови демократичної, правової, соціальної держави [27, с.16].

Сьогодні для того, аби захистити державу від негативного інформаційного впливу, особливу увагу необхідно приділити таким видам небезпек, як: витіснення українських інформаційних агенцій, ЗМІ з внутрішнього інформаційного ринку, подолати залежність економічної та політичної сфери суспільного життя України від іноземних інформаційних структур. Також необхідно витіснити маніпулювання інформацією, що включає приховування або перекручення інформації, дезінформацію тощо [22, с. 240].

Однією з проблем інформаційної безпеки наразі вважаються кіберзлочини на внутрішньому ринку. Помітної шкоди завдають комп'ютерні злочини, направлені на мережі банківських установ і кредитних спілок. Основною метою кібер-зловмисників є не самі банки, а їхні клієнти, і зловмисник може використовувати їхню некомпетентність.

Серед основних завдань захисту держави від інформаційно-психологічних загроз можна назвати захист від деструктивних інформаційних впливів суспільства і соціальних груп громадян, відстоювання національних інтересів України в інформаційному просторі, а також протидію спробам маніпулювання за рахунок інформації з боку ворожих для держави політичних сил.

Зазначимо, що для того, аби створити систему забезпечення інформаційної безпеки держави, необхідно правильно сформувати її мету. Вона передбачає створення необхідних економічних і соціо-культурних умов, а також правові організаційні механізми формування ефективного використання інформаційних ресурсів у всіх сферах життя суспільства [18].

На думку окремих вчених, з якими ми цілком погоджуємося, головним стратегічним завданням реалізації та захисту національних інтересів на сучасному етапі розвитку України в інформаційній сфері стають:

1) розробка довгострокової програми щодо забезпечення виходу на рівень провідних країн світу у сфері створення новітніх інформаційних технологій;

2) свобода отримання і поширення інформації громадянами в інтересах суспільства, розвитку науки та культури;

3) безпечний захист інформаційного потенціалу нашої країни від неправомірного його використання задля шкоди інтересам особистості, суспільства й держави;

4) взаємодія державних і недержавних систем інформаційного забезпечення з метою найбільш ефективного використання інформаційних ресурсів держави;

5) протидія планомірним діям щодо дезінформації органів влади та використання каналів інформаційного обміну для порушення систем управління різними сферами життєдіяльності держави

6) формування і розвиток регіональних центрів сертифікації систем інформаційного захисту та їх елементів; [36, с. 108-109].

На нашу думку, для того, аби досягти відповідного рівня інформаційної безпеки необхідно сформувати єдиний державний механізм забезпечення інформаційної безпеки України, де будуть вирішуватися такі основні завдання:

1) забезпечення інформаційної безпеки та складових елементів системи управління державної безпеки;

2) розвиток і розробка ефективної системи отримання потрібної інформації для відпрацювання оперативних стратегічних і тактичних рішень у сфері управління інформаційною безпекою;

3) формування інформаційно-аналітичного потенціалу країни;

4) розвиток системи контролю стану інформаційної безпеки у зв'язку з виявленням небезпек, які виникають як зсередини, так і ззовні системи управління національною безпекою;

5) запобігання будь-якій протиправній діяльності з боку суб'єктів інформаційної системи у сфері забезпечення національної безпеки.

До функцій системи забезпечення інформаційної безпеки країни можна віднести, по-перше, планування, куди включаються виявлення, моніторинг, прогнозування загроз національним інтересам, по-друге, координацію, тобто визначення і здійснення повноважень системою управління національної безпеки, по-третє, стимулювання, тобто розробку і реалізацію політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами, по-четверте, контроль за станом, поряд-ком і правилами формування, розвитку і використання інформаційних ресурсів, по-п'яте, державне регулювання сфери інформатизації щодо забезпечення науково-технічних і організаційно-економі чеських умов створення та застосування інформаційних технологій.

Серед інститутів, що гарантують інформаційну безпеку, можна виокремити верховенство закону, незалежний і компетентний суд, відсутність корупції тощо [15, с. 9]. Інституційний механізм забезпечення інформаційної безпеки є особливою структурною складовою частиною державного механізму, що забезпечує створення норм і правил регулювання взаємодії різних економічних суб'єктів в інформаційній сфері щодо запобігання загроз інформаційній безпеці.

Інституційний механізм приводить у дію інститути (формальні і неформальні), структурує взаємодії суб'єктів, які здійснюють контроль над дотриманням встановлених норм і правил.

Сутність інституційного механізму виявляється через його функції. Ми вважаємо, що інституційний механізм виконує такі функції, які можна застосувати й до механізму забезпечення інформаційної безпеки, а саме:

– інтеграцію агентів в один інститут з метою здійснення спільної діяльності в рамках загальних статусів і норм;

– диференціювання норм і статусів, а також суб'єктів і агентів різних інститутів, що розділяють та ігнорують їхні вимоги;

– застосування нових вимог у реальну практику;

– субординацію і координацію відносин між суб'єктами, які належать до різних інститутів;

– інформування суб'єктів про нові норми і правила поведінки;

регулювання діяльності суб'єктів;

– контроль за виконанням норм, правил [46, с. 144].

Таким чином, інституційний механізм забезпечення інформаційної безпеки включає законодавчу основу і забезпечує її інституційні елементи. Покращання цього механізму передбачає реорганізацію законодавчої основи інформаційної безпеки та інституційних структур протидії загрозам

інформаційній безпеці. До інституційного механізму забезпечення інформаційної безпеки входить:

– прийняття нових законів, які враховували б інтереси всіх суб'єктів інформаційної сфери;

– дотримання балансу творчої та обмежувальної функцій законів в інформаційній сфері;

– інтеграція України у світовий правовий простір;

– облік стану сфери вітчизняних інформаційних технологій тощо.

Слід констатувати, що державна інформаційна політика повинна відбивати нагальні питання, що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Найскладнішими тут є такі завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави і суспільства з одночасним виокремленням нагальних пріоритетів, до яких слід віднести створення / відновлення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію наведених вище механізмів створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності.

Отже, національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури. Питання вирішення забезпечення механізмів у сфері інформаційної безпеки потребує подальшого глибоко вивчення.

ВИСНОВКИ

Сьогодні питання національної безпеки дедалі більше перетинаються з питаннями глобальної безпеки і відповідно повинні вирішуватися в рамках партнерства і співпраці. Найбільш важливою сферою такої співпраці є забезпечення національної й міжнародної інформаційної безпеки.

У ході нашого дослідження ми визначили основні поняття й підходи до вивчення політичного інформаційного простору, охарактеризували концепції «інформаційної війни» у вітчизняній та зарубіжній політології.

Ми встановили, що інформаційна війна є багатоплановим і достатньо складним феноменом, що ведеться в різних вимірах.

Також нами розглянуто форми, види і методи ведення інформаційних війн на сучасному етапі. Крім того нам вдалося проаналізувати проблему інформаційної безпеки України в умовах сучасних інформаційних війн і визначити загрози безпеці нашої держави в інформаційній сфері. Насамкінець ми визначили механізми забезпечення інформаційної безпеки України.

Підсумовуючи зазначене, можемо зробити наступні висновки.

Для вироблення національної політики в сфері забезпечення інформаційної безпеки перш за все необхідна тверезa оцінка сьогоднішнього стану, особливостей і перспектив розвитку інформаційної зброї і засобів її застосування. Така оцінка є базовою передумовою для вироблення зовнішньої і внутрішньої політики держави, військові і військово-технічні компоненти якої могли б запобігати виникненню загроз і надійно забезпечили б безпеку країни.

При цьому важливо зрозуміти, що загроза інформаційної війни і інформаційної злочинності в широкому контексті є фактор прихованого воєнно-політичного тиску і залякування, фактор, що здатен порушити світову

і регіональну стабільність і безпеку. Саме тому в широкому плані повинен здійснюватися моніторинг загроз застосування інформаційної зброї та перманентна оцінка ефективності функціонування систем протидії цієї зброї.

Такий моніторинг має охоплювати не лише науково-технічні і технологічні досягнення в розробках інформаційної зброї та засобів протидії їй, але і динаміку передумов і умов її можливого застосування, тобто, змін зовнішньо-політичної ситуації, прогноз глобальних і локальних протиріч і конфліктів, котрі несуть за собою загрозу інформаційної війни.

Природньо було б відслідковувати такі стани внутрішнього і міжнародного законодавчого і нормативно-правового забезпечення інформаційної безпеки.

Вирішення проблеми інформаційних загроз країні дасть змогу забезпечити захист інтересів суспільства і держави, гарантуватиме право громадян на отримання якісної та об’єктивної інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про основи національної безпеки України» / Відомості Верховної Ради України, 2003. – № 39, ст. 351 // Голос України. – 22 липня 2003 року.

2. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 року № 555/2015 // Урядовий кур'єр. – № 178, 26 вересня 2015.

3. Про Концепцію розвитку сектору безпеки і оборони України: Указ Президента України від 14.03.2016 р. № 92/2016 // Урядовий кур'єр. – № 52. – 18 березня 2016.

4. Про стратегію національної безпеки України: Указ Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015.

5. Аронсон Э., Пратканис Э. Эпоха пропаганды: Механизмы убеждения, повседневное использование и злоупотребление. СПб.: прайм-ЕВРОЗНАК, 2003. – 384 с.

6. Аюрова А. М. Информационная война как феномен информационного общества. Экспериментальные и теоретические исследования в современной науке: сб. ст. по матер. II междунар. науч.-практ. конф. № 2(2). Новосибирск: СибАК. –2017. – С. 67-76.

7. Буньківська О.В. Вплив інноваційних інформаційних технологій на функціонування національного інформаційного простору / О.В.Буньківська // Фундаментальні і прикладні дослідження рекреаційно-дозвіллєвої сфери в контексті євроінтеграційних процесів: зб.матеріалів Міжнарод. науково-практ. конф. – К.:КНУКіМ, 2008. – С.54 – 61.

8. Бухарин С. Н., Цыганов В. В. Информационные войны в бизнесе и политике. М., 2007. –336 с.

9. Волкогонов Д. А. Психологическая война. М., 1984. – 320 с.

10. Гойман О. О. Маніпулювання масовою свідомістю в умовах сучасної гібридної війни [Електронний ресурс] / О. О. Гойман // Грані. – 2015. – № 1. – С. 50-56.

11. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань // Вісник Національної академії державного управління при Президентові України. – 2015. – № 1. – С. 136-141. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21

12. Грани глобализации: Трудные вопросы современного развития. – М.: Альпина Паблишер, 2003. – 67 с.

13. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. М., 2004. – 428 с.

14. Гриняев С. Концепция ведения информационной войны в некоторых странах мира. URL: http://www.soldiering.ru/psychology/conception_psywar.php

15. Добровольська А.Б. Інформаційний простір: проблеми становлення нової якості національного росту / А.Б. Добровольська // Наука України у світовому інформаційному просторі. – Вип. 3. – К.: Академперіодика, 2010. – С. 61-70

16. Жарков Я.М., Присяжнюк М.М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування // Вісн. Київ. нац. ун-ту імені Тараса Шевченка. Сер. Військово-спеціальні науки. – 2007. – №14 –15. – Вип. 14. – С. 42 – 44.

17. Здоровега В.Й. Українська періодика у сучасному національному інформаційному просторі // Українська періодика: історія і сучасність. – Львів, 1995. – С. 11-18.

18. Зиновьев А. Глобализация как война нового типа. URL: http://www. intelros.org/lib/statyi/zinoviev1.htm

19. Зозуля О. С. Інформаційна зброя як геополітичний чинник та інструмент силової політики [Електронний ресурс] / О. С. Зозуля // Державне управління: теорія та практика. – 2013. – № 2. – С. 82-89. – Режим доступу: http://nbuv.gov.ua/UJRN/Dutp_2013_2_12 – Назва з екрана.

20. Іванов В. Основні теорії масової комунікації і журналістики: навч. посіб. / В. Іванов; За науковою редакцією В.В. Різуна. – К.: Центр Вільної Преси, 2010. – 258 с

21. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

22. Історія інформаційно-психологічного протиборства: підруч. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш; за заг. ред. д.ю.н., проф., засл. юриста України Є. Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.

23. Караяни А. Г. Теория и практика психологической войны. Организация и проведение информационных операцій. Официальный сайт библиотеки «Psyfactor». URL: http://psyfactor.org/lib/psywar30.htm

24. Карпенко В. Інформаційний простір як чинник національної безпеки України. Українознавство: науковий громадсько-політичний культурно-мистецький релігійно-філософський педагогічний журнал. 2005. – № 3. С. 182-192.

25. Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах [Електронний ресурс] / М. О. Кондратюк // Вісник

Харківської державної академії культури. – 2013. – Вип. 41. – С. 108-113. – Режим доступу: http://nbuv.gov.ua/UJRN/hak_2013_41_15

26. Костюк І. А. Інформаційні війни в контексті революційних подій в Україні. Актуальні проблеми соціальних комунікацій: матеріали студентської наукової конференції, 22 травня 2014 р. Київ, 2014. С. 57-60.

27. Левченко О.В. Еволюція гібридної війни Російської Федерації проти України / О.В. Левченко // Наука і оборона. – 2017. – № 2. – С. 11-16.

28. Лібікі М. Що таке інформаційна війна? / М. Лібікі [Електронний ресурс]. – Режим доступу: http://viysko.com.ua/texnologiji-voyen/martin-libiki-shho-take-informacijna-vijna/

29. Литвиненко О. В., Бінько І.Ф., Потіха В. М. Інформаційний простір як чинник забезпечення національних інтересів України. – К.: – Чорнобильінформ. –1998. – С. 13, 21 – 22, 48.

30. Людендорф Э. Мои воспоминания о войне 1914-1918 годов. М., 2015. – 448 с.

31. Манойло А. В. Государственная информационная политика в особых условиях. М. – 2013. – 388 с.

32. Матвеичев О. «Мягкая сила» против атомной бомбы. М.: Книжный мир, 2016. – 352 с.

33. Медведєв В. К. Сучасна інформаційна війна та її обрис [Електронний ресурс] / В. К. Медведєв, Ю. Ф. Кучеренко, Р. М. Гузько // Системи озброєння і військова техніка. – 2008. – № 1. – С. 52-54. – Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2008_1_13

34. Михальченко И. А. Информационные войны на рубеже XXI века. Безопасность информационных технологий. 1998. – № 3. – С. 14-15.

35. Павлютенкова М. Ю. Информационная война: реальная угроза или современный миф? Власть. 2001. –№ 12. – С. 19-23.

36. Панарин И. Н. Информационная война и третий Рим. М. – 2001. – 244 с.

37. Панарин И.Н. Информационная война и геополитика / И. Н. Панарин // Изд-во: Русское слово. – М. – 2009. – 466с.

38. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки / Г.В. Пєвцов, С.В. Залкин, А.О. Феклістов // Інформаційна безпека. – 2011. – № 2. – С. 57-59.

39. Политические коммуникации / Под ред. А. И. Соловьева. – М., 2004. – 231 с.

40. Поняття інформаційного простору [Електронний ресурс] // Навчальні матеріали онлайн. – Режим доступу: http://pidruchniki.-com/1350052747708/informatika/ponyattya_- informatsiynogo_prostoruю/

41. Потехин В.К. Современные войны и национальная безопасность России // Кому будет принадлежать консциентальное оружие в XXI веке? М., 1997. – С. 69-87.

42. Почепцов Г.Г. Стратегический анализ. Стратегический анализ для политики, бизнеса и военного дела / Г.Г. Почепцов. – Л.: Дзвін, 2004. – 333 с.

43. Почепцов Г.Г. Информационные войны. Новый инструмент политики. М.: Алгоритм, 2015. – 256 с.

44. Почепцов Г. Г. Психологические войны / Г. Г. Почепцов. – К.: Рефл-бук, Ваклер, 2000. – 529 с.

45. Почепцов, Георгій. Сучасні інформаційні війни. – Вид. 2-ге, доповнене. – К.: Вид. дім «Києво-могилянська академія», 2016. – 504 с.

46. Расторгуев С. П. Информационная война. М. – 1998. –222 с.

47. Різун В.В. Теорія масової комунікації. Підручник / В. В. Різун – К.: Просвіта, 2008. – 260 с.

48. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. Вісник Книжкової палати. 2013. № 1. С. 40-43.84 Актуальні проблеми політики. 2018. Вип. 61

49. Соловей В.Д. Абсолютное оружие. Основы психологической войны и медиаманипулирования. М., 2016. – 320 с.

50. Соснін О. В., Олійник О. В. Правові проблеми регулювання інформаційної діяльності / О. В. Соснін, О. В. Олійник // Стратегічна панорама. – 2002. – № 4. – С. 166-174.

51. Тоффлер Э. Третья волна (текст) / Э. Тоффлер / Пер. с англ. О.А. Феофанова. – М.: Акма-пресс, 1999. – 654 с.

52. Цыганов В.В. Информационные войны в бизнесе и политике: Теория и методология. М.: Академический Проект, 2007. – 336 с.

53. Швец Д. А. Информационное управление как технология обеспечения информационной безопасности. Массовая коммуникация и массовое сознание. М. – 2003. – 34 с.

54. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. Демократичне врядування. 2014. Вип. 13. URL: http:// lvivacademy.com/visnik13/zmist.html

55. Шпига П.С., Рудник Р.М. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. – 2014. Вип. 8. С. 326-339.